

## **Pinkerton Academy Acceptable Use Policy for Digital and Electronic Media Communication for Faculty/Staff**

As a school whose vision is to *encourage innovation in response to a changing world* and whose goal is to promote *educational excellence in a challenging, respectful and collaborative environment*, Pinkerton Academy realizes that part of 21<sup>st</sup> century learning is adapting to changing methods of communication. Major components of this include social media and web 2.0 tools. Social media can be defined as any online tool and/or service that allow any Internet user to create and publish content online. Examples of social media tools include but are not limited to Edmodo, Facebook, Ning, Twitter, YouTube, blogs, wikis, etc. Web 2.0 can be defined as user-oriented web applications, which are interactive and collaborative in nature. [Click here](#) or visit <http://edudemic.com/2011/11/best-web-tools/> for a list of web 2.0 tools used by educators.

The importance of teachers, staff, students, and parents engaging, collaborating, learning, and sharing with these various digital communication tools is a part of the 21<sup>st</sup> century learning environment. For the purpose of education and instruction, clear boundaries, which promote positive and appropriate relationships among all members of the Pinkerton Academy community (students, faculty and staff, parents, and administration), create an atmosphere of trust and individual accountability and responsibility. Being digitally responsible means adhering to the same professional standards of conduct that are expected in face to face communication. Pinkerton Academy employees should be familiar with the following Acceptable Use Policy. ***Any violation of these guidelines will be grounds for disciplinary action, up to and including termination of employment. In addition, any violation of this policy may result in suspension or revocation of a staff member's technology privileges, referral to law enforcement and/or legal action. Any member of the staff or faculty who intentionally damages the Academy's computer system or network shall assume legal and financial liability for such damage.***

The Academy's technology remains under the control, custody, and supervision of the Academy at all times. The Academy reserves the right to monitor all use of its computers, email, Internet/Intranet, iPads, iPods, laptops, and other technology. Faculty and staff have no expectation of privacy in their use of Academy technology.

Faculty and staff who use Academy technology with students are responsible for supervising such student use. Faculty and staff are expected to be familiar with the Academy's policies and rules concerning student technology and internet use, and are required to enforce those policies and rules.

### **Acceptable Use for Faculty and Staff:**

Each faculty and staff member is responsible for his/her actions and activities involving all Academy and personal technological devices used at school or at a school function, including but not limited to, networks, Internet/Intranet, stand-alone workstations, laptops, iPods, iPads, cell phones, and other technology. This policy does not describe every possible permitted or prohibited activity. Faculty and staff who have questions about whether a particular activity is permitted or prohibited are encouraged to contact an administrator.

Any system which requires password access shall only be used by the authorized user. Faculty and staff shall not share passwords or other login information with other users. Account owners are responsible for all activity under their accounts.

- Pinkerton Academy faculty and staff (hereafter referred to as “employees”) are personally responsible for the content they publish online.
- Online communication, interactions, and behaviors should reflect the same standards of honesty, respect, and consideration that you use for face to face communication. (*See Professional Conduct, Professional Staff Handbook, pages 16-17*)
- Employees’ on-line relationships with students will align with the guidelines set fourth in the professional staff handbook. (*See Professional Conduct, Professional Staff Handbook, pages 16-17*)
- Employee will not disclose confidential information or post things that are disparaging of the Academy (*Professional Staff Handbook, page 17*) or in regards to any members of its community (students, other faculty/staff, parent/guardians). Employees will not use the Internet, social media and/or Web 2.0 tools to put other students or the Pinkerton community as a whole at risk or in a manner that would jeopardize the safety of the Pinkerton community.
- Employees will model appropriate behavior and will exercise their professional judgment when using digital communication and resources.
- Employees are expected to model and promote digital responsibility by emphasizing on-line safety through the use of appropriate privacy settings.
- All Pinkerton Academy employees are expected to abide by the school policies and ensure safe and ethical relationships with all members of the school community; this includes but is not limited to social media and web 2.0 tools. (*Professional Staff Handbook, pages 16-17, 26*)
- Employees are encouraged to use social media and web 2.0 tools provided they follow the Acceptable Use Policy for faculty and staff.
- All hardware and software is either owned or licensed by Pinkerton Academy. All users are required to use the hardware and software in accord with its designed purpose. No hardware or software shall be altered or reconfigured without the permission of the administration.

**Unacceptable Uses for Faculty and Staff.** Unacceptable use activities include, but are not limited to, any activity through which the user:

- Uses the Academy’s technology to violate the acceptable uses set forth above.
- Creates, accesses, submits, posts, publishes, forwards, downloads, scans, or otherwise displays defamatory, abusive, obscene, vulgar, threatening, discriminatory, harassing, and/or illegal materials.
- Uses the Academy’s computers or other technological devices, networks, or internet/intranet for any illegal activity, or in violation of any Academy policy or rule, such as for bullying, cyberbullying, harassing, and vandalizing, or in support of such activities.
- Violates copyrights, license agreements, and/or contracts.
- Plagiarizes.
- Engages in malicious use, disruption, or harm to the Academy’s computers or other technological devices, networks, or internet/intranet, including but not limited to hacking and creating/uploading computer viruses and/or worms.
- Engages in inappropriate communications with students or minors.
- Represents his/her personal views as those of the Academy, or communications that could be misinterpreted as such.
- Downloads or installs software or other applications without permission from the administration.
- Accesses or attempts to access confidential information stored on the Academy’s network or server.
- Fails to report a breach of the technology security system to the administration.
- Uses Academy technology after such access has been denied or revoked.

- Attempts to access unauthorized websites, or attempts to disable or circumvent the Academy's filtering/blocking technology (unless a filter override has been authorized by the administration).
- Misuses or damages the Academy's technology equipment, including but not limited to, opening and forwarding email attachments from unknown sources and/or that may contain viruses.
- Maliciously uses or disrupts the Academy's computers or other technology devices, networks, or internet/intranet services, including but not limited to, the misuse of computer passwords or accounts, misrepresenting oneself as another user, and/or unauthorized access of another user's folders, work, files or emails.
- Uses the Academy's technology for any other use that is inconsistent with the Academy's educational mission and/or is not for educational purposes.

***Any violation of these guidelines will be grounds for disciplinary action, up to and including termination of employment and may result in suspension or revocation of the employee's technology privileges, referral to law enforcement and/or legal action.*** If you have any questions or concerns, please see or submit the questions or concerns in writing to the administration.

Approved by Board of Trustees  
June 20, 2013